

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

FILED
RICHARD W. NAGEL
CLERK OF COURT

2019 MAY -1 PM 3:16

U.S. DISTRICT COURT
SOUTHERN DISTRICT
OF OHIO
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF
THE CELLULAR TELEPHONE ASSIGNED
CALL NUMBER **702-569-9982** SERVICED
BY AT&T WIRELESS

Case No. **1:19MJ-327**

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Paul W. Cox, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A) for information about the location of the cellular telephone assigned call number **702-569-9982** (the “**Target Cell Phone**”), whose service provider is **AT&T WIRELESS**, a wireless telephone service provider headquartered at **11760 US Highway 1, Suite 600, North Palm Beach, FL 33408**. The **Target Cell Phone** is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. Because this warrant seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a “pen register” and/or “trap and trace device,” *see* 18 U.S.C. § 3123(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. *See* 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. *See* 18 U.S.C. § 3123(b)(1).

3. I am a Special Agent for the Food and Drug Administration-Office of Criminal Investigations (“FDA-OCI”). I am currently assigned to the Kansas City Field Office, and am the Seized Computer Evidence Recovery Specialist/Computer Forensics Agent for the Kansas City

Region. My current duties include investigating violations of the Federal Food Drug and Cosmetic Act and other violations of the United States Criminal Code. I have been employed as a Special Agent since November 2012. Prior to my current position with FDA-OCI, I was employed as a Special Agent with the Department of Health and Human Service ("HHS") Office of Inspector General Computer Crimes Unit, stationed at the Centers for Disease Control and Prevention and the HHS Computer Security Incident Response Center, and prior to that I was a Special Agent with the National Aeronautics and Space Administration-Office of Inspector General ("NASA-OIG") Computer Crimes Division, stationed at the Jet Propulsion Laboratory. I am a graduate of the following training programs: Criminal Investigator Training Program and the Seized Computer Evidence Recovery Specialist Program at the Federal Law Enforcement Training Center (2013), Inspector General Criminal Investigator Academy (2014), HHS Special Agent Basic Training Program (2016), and the FDA-OCI Special Agent Training Program (2018). During my career, I have received specialized training in the investigation of computer crimes, combating the distribution of child pornography, the performance of digital forensics, and investigating the sale of counterfeit, adulterated, and misbranded drugs via the internet and dark web. Additionally, I have presented training to other federal law enforcement officers in the United States on the topic of cyber investigations and have presented training on the investigation of the online sale of counterfeit drugs to international law enforcement officials at the Interpol Global Complex for Innovation in Singapore. Through the course of my duties, I have conducted numerous investigations into the distribution of counterfeit, misbranded, and adulterated drugs and controlled substances via the dark web and United States Postal Service, and personally executed approximately 30 undercover purchases of drugs via the dark web in exchange for cryptocurrency. Through the course of my duties I have participated in the execution of numerous search warrants.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code, Sections 841(a)(1), 846, 331(a), 331(k), and 331(i), and Title 18, United States Code, Section 1957 have been committed and are being committed by Khlari Sirotkin and unknown persons. There is also probable cause to believe that the location information described in Attachment B will constitute evidence of these criminal violations, and will lead to the identification of individuals who are engaged in the commission of these offenses.

6. The court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. FDA-OCI is investigating the distribution of counterfeit and misbranded opiate-based prescription drugs by a seller using the moniker “Pill-Cosby” and “SlangGang” on Darknet Marketplace known as Dream Market, Wall Street, and Empire Market. From a series of undercover purchases, I have learned that all of the drugs sold by Pill-Cosby and SlangGang are sent through the USPS, using postage paid for using Bitcoin cryptocurrency. Furthermore, records of the purchases of items used in the manufacture of counterfeit drugs indicate that Sirotkin has purchased several items consistent with counterfeit drug manufacturing, and that Sirotkin utilizes his mobile phone and email accounts in furtherance of his drug trafficking organization.

8. Over the past year, FDA-OCI, working with the Drug Enforcement Administration, the United States Postal Inspection Service, the Federal Bureau of Investigation, and Homeland Security Investigations have been investigating opiate-based prescription drugs being advertised and sold on Darknet Marketplaces, and distributed through the USPS.

9. From my participation in this investigation, my knowledge, training and experience, my review of investigation reports by other members of the investigative team and discussions with other federal agents involved in the investigation of individuals involved in the distribution of misbranded and counterfeit opiate-based prescription drugs via the USPS, I know the information included in the following paragraphs.

I. Investigation of “Pill-Cosby” and “SlangGang”

10. Between April 2018 and April 2019, agents from the Food and Drug Administration -- Office of Criminal Investigations (FDA-OCI), the Federal Bureau of Investigations (FBI), the United States Postal Inspection Service (USPIS), Homeland Security Investigations (HSI), and the Drug Enforcement Administration (DEA) have been conducting an investigation into the manufacture and distribution of counterfeit oxycodone tablets originating from the Las Vegas-area, sold via the darkweb marketplaces Dream Market, Wall Street Market, and Empire Market in exchange for Bitcoin cryptocurrency, and distributed via the United States Postal Service.

11. A review of the vendor pages on Dream Market, Wall Street Market, and Empire Market has shown that the vendor Pill-Cosby has been active since September 2017 and is responsible for over 5,800 transactions with an estimated \$2.35M (USD) in sales, and that SlangGang has been active since June 2018 and is responsible for over 1,100 transactions with an estimated \$235,000 (USD) in sales.

12. During the course of this investigation, ten (10) undercover purchases have been made from the monikers SlangGang and Pill-Cosby between April 2018 and April 2019, including

purchases delivered to the Southern District of Ohio. In each of these undercover purchases, agents placed an order for counterfeit oxycodone tablets in exchange for Bitcoin cryptocurrency. In each of these instances the drugs were purchased without a valid prescription and they were dispensed in packaging that did not bear proper instructions for use or warnings. In the case of each purchase, an undercover agent placed an order for counterfeit oxycodone pills in exchange for Bitcoin cryptocurrency, and provided an undercover address to which the purchase was to be delivered.

13. In each case, agents subsequently received parcels to the undercover addresses provided at the time of the purchases. These parcels contained items matching the description of the items purchased by the undercover agent. The contents included tablets, of various quantities, blue in color, round in shape, bearing pill imprints "A 215" and a half-tablet score mark. The parcels were all found to bear postage purchased from the USPS reseller EasyPost, and originated from the Las Vegas, Nevada, area.

14. Based on my training and experience, I know that the pill imprint A 215 is associated with a 30 mg oxycodone HCL tablet sold by Actavis. I also know that oxycodone HCL is a Schedule II controlled substance.

15. A review of USPS databases indicates that all of the parcels received following purchases from Pill-Cosby and SlangGang were purchased by an EasyPost postage meter associated with BitcoinPostage.info. Based on my training and experience, I know BitcoinPostage.info to be a service which sells postage in exchange for Bitcoin. I further know that individuals involved in the distribution of narcotics on the darkweb in exchange for cryptocurrency utilize services like BitcoinPostage.info in order to avoid the currency exchange from Bitcoin to fiat currency and to conceal their illegal activities.

16. Additionally, a review of the return addresses found on the parcels received following purchases from Pill-Cosby and SlangGang show that these parcels consistently bear

return addresses including the phrase "EBAY FULFILLMENT." Based on my training and experience, I know that individuals involved in the distribution of large quantities of drugs using the United States Postal Service often utilize fraudulent return addresses to appear consistent with legitimate businesses with a high volume of mailings, in order to hide their activity from law enforcement.

17. Specifically, on December 04, 2018, FDA-OCI agents acting in an undercover capacity placed an order for fifteen (15) pills advertised as "Pressed 30mg Oxy \$13 each." On December 11, 2018, investigators from the DEA and USPIS retrieved a parcel from the undercover address provided at the time of this purchase. The parcel contained fifteen (15) tablets, blue in color, round in shape, bearing the pill imprint "A 215" and a half tablet score. Additionally, the parcel containing the pills was found to bear postage purchased from EasyPost, and originated from the Las Vegas, Nevada, area. A review of USPS databases indicates that these parcels were purchased by an EasyPost postage meter associated with BitcoinPostage.info. Subsequent analysis of these pills indicated that these pills did not contain oxycodone HCL but rather, contained fentanyl.

18. All of the parcels received following the purchase of pills from Pill-Cosby and SlangGang were found to contain pills packaged in a similar fashion and contained pills of similar shape, color, size, and bearing the pill imprint "A 215" and a half tablet score.

19. Records provided by Paypal, Inc., indicate that between on or about January 27, 2017 and on or about April 25, 2017, a Paypal account with ID #: ending in 4715 was used to send approximately \$3,800 (USD) in exchange for multiple items used in the manufacture of counterfeit drugs. Specifically, Paypal account ending in 4715 was used to purchase items with the following descriptions: "Handheld Manual Tablet Press Pill Maker TDP-00 making pills/tablet No die mould", "6mm A/215 Punching Die Mold Stamp for candy tablet press mold pill maker

[TDP0/1.5]”, “Automatic Electric Single Punch Tablet Press Pill Pellet Making Machine TDP-5”, and “TDP-5 Tablet Press Machine 5000 Tablets/Hour Prompt Services Easy Maintenance.”

20. Based on my training and experience, I know that it is common for individuals involved in the sale of counterfeit punches and dies to advertise them as having an intended use for the manufacture of candy or confections in order to conceal their activity from law enforcement. I also know that a TDP-5 tablet press, manufactured by LFA Machines Oxford LTD, is a 5 ton desktop tablet press capable of producing 5,000 tablets per hour.

21. A review of records related to Paypal account ending in 4715 show that the account was registered in the name KHLARI ISBELL SIROTKIN, social security number ending in -6210, Date of Birth (DOB) XX/XX/1983, the address 6260 REDWOOD LAS VEGAS, NV 89118, the telephone numbers 702-91-1148 ¹ [sic] and **(702) 569-9982 (the Target Cell Phone)**, and the email address KLIZOSIROTA@GMAIL.COM.

22. Additionally, Paypal records indicate that Paypal account # ending in 3777 was registered in the name KHLARI SIROTKIN at the address 2735 W PEBBLE RD UNIT 313 LAS VEGAS, NV 89123, and the email address KLIZOB@GMAIL.COM.

23. Based on my training and experience, companies like Paypal communicate with their customers regarding records of transactions using the phone provided by the customer at the time of account registration. I therefore believe that the **Target Cell Phone** is used by SIROTKIN aka “Pill-Cosby” aka “SlangGang” in the commission of the criminal conduct described herein, and that the locations provided will yield evidence of crime, fruits of crime and [other] instrumentalities of crime.

¹ At present, it is believed that this was a typo and that this number was intended to be the number indicated as 702-901-1148.

24. In my training and experience, I have learned that **AT&T Wireless** is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including E-911 Phase II data, also known as GPS data or latitude-longitude data and cell-site data, also known as “tower/face information” or cell tower/sector records. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device’s signal using data from several of the provider’s cell towers. [Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the “sector” (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise than E-911 Phase II data.

25. Based on my training and experience, I know that **AT&T Wireless** can collect E-911 Phase II data about the location of the **Target Cell Phone**, including by initiating a signal to determine the location of the **Target Cell Phone** on **AT&T Wireless**’s network or with such other reference points as may be reasonably available.

26. Based on my training and experience, I know that **AT&T Wireless** can collect cell-site data about the **Target Cell Phone**. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower

to which the customer connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as **AT&T Wireless** typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

AUTHORIZATION REQUEST

27. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c).

28. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the **Target Cell Phone** would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

29. I further request that the Court direct **AT&T Wireless** to disclose to the government any information described in Attachment B that is within the possession, custody, or control of **AT&T Wireless**. I also request that the Court direct **AT&T Wireless** to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the

information described in Attachment B unobtrusively and with a minimum of interference with **AT&T Wireless's** services, including by initiating a signal to determine the location of the **Target Cell Phone** on **AT&T Wireless's** network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate **AT&T Wireless** for reasonable expenses incurred in furnishing such facilities or assistance.

30. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the Target Cell Phone outside of daytime hours.


31. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



Paul W. Cox
Special Agent
Food and Drug Administration-Office of
Criminal Investigations

Subscribed and sworn to before me on this 1 day of ^{May}~~April~~, 2019



Honorable Stephanie K. Bowman
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

1. The cellular telephone assigned call number **702-569-9982** (the “**Target Cell Phone**”), whose wireless service provider is **AT&T Wireless**, a company headquartered at **11760 US Highway 1, Suite 600, North Palm Beach, FL 33408**.
2. Records and information associated with the **Target Cell Phone** that is within the possession, custody, or control of **AT&T Wireless**, including information about the location of the cellular telephone if it is subsequently assigned a different call number.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

All information about the location of the **Target Cell Phone** described in Attachment A for a period of thirty days, during all times of day and night. “Information about the location of the **Target Cell Phone**” includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, as well as all data about which “cell towers” (i.e., antenna towers covering specific geographic areas) and “sectors” (i.e., faces of the towers) received a radio signal from the cellular telephone described in Attachment A.

To the extent that the information described in the previous paragraph (hereinafter, “Location Information”) is within the possession, custody, or control of **AT&T Wireless**, **AT&T Wireless** is required to disclose the Location Information to the government. In addition, **AT&T Wireless** must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with **AT&T Wireless**’s services, including by initiating a signal to determine the location of the **Target Cell Phone** on **AT&T Wireless**’s network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate **AT&T Wireless** for reasonable expenses incurred in furnishing such facilities or assistance.

This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

II. Information to Be Seized by the Government

All information described above in Section I that constitutes evidence of violations of Title 21, United States Code, Sections 841(a)(1), 846, 331(a), 331(k), and 331(i), and Title 18, United States Code, Section 1957 involving Khlari Sirotkin and unidentified subject(s).